How to Configure MSAD Authentication

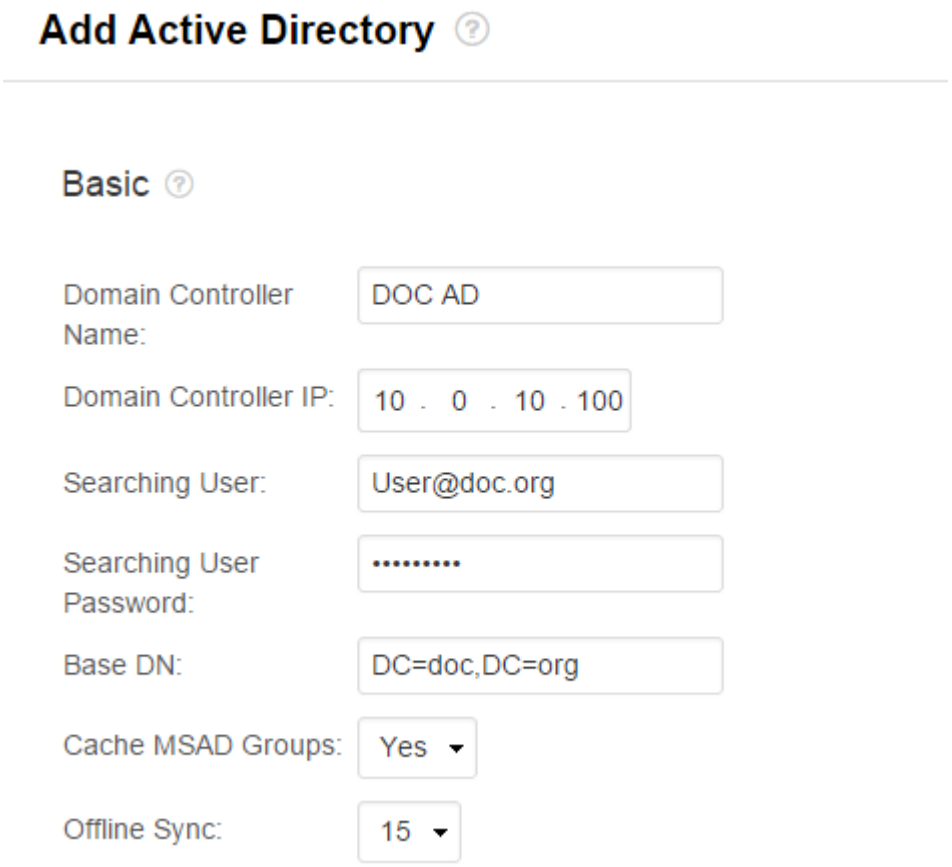
https://campus.barracuda.com/doc/43224170/

Configure the Barracuda NextGen Firewall X-Series to allow authentication and authorization of domain users on a Microsoft Active Directory (MSAD) server. To reduce load querying for large environments, you can also filter unwanted group membership information by creating group filter patterns.

Configure MSAD Authentication

Connect the X-Series Firewall with your Microsoft Active Directory (MSAD) server and configure MSAD as external authentication scheme.

1. Go to the **USERS** > **External Authentication** page.
2. Click the **Active Directory** tab.
3. In the **Basic** section, click **Add**.
4. Enter the **Domain Controller IP** address.
5. In the **Searching User** field, enter the MSAD **Searching User** in the `user@domain` format:
   Do not use the `domain\user` format.
6. Enter the **Searching User Password**.
7. Specify the **Base DN** where the lookup should be started. E.g., `CN=trainee,OU=sales,DC=mycompany,DC=com`
   Do not use spaces between the entries.
8. Set **Cache MSAD Groups** to **Yes** to reduce network traffic and server load on the domain controller.



9. Select **Use SSL** if your Active Directory server is configured to use SSL.
10. (Optional) Select **Follow Referrals** to use Active Directory's global catalog and follow the referrals. When a requested object exists in the directory but is not present on the contacted domain controller, the referral gives the client a location that holds the object or is more likely to hold the object. It is also possible for the referred-to domain controller to refer to a next hop location. The number of next hops is defined in **Maximum Hops for Referrals**.
11. Click **Save**.
12. (Optional) Add **Group Filter Patterns** to filter unwanted group information. Wlldcards are allowed.
    Example: When using pattern: **SSL**, and the following group membership strings are used:
    User01 group membership string: `CN=xyz,OU=sales,DC=mycompany,DC=com`
    User02 group membership string: `CN=SSL,DC=mycompany,DC=com`
    Only **User02** will match.
13. Click **Save**.

The configuration is now added to the **EXISTING AUTHENTICATION SERVICES** table and you can use the MSAD authentication service on the X-Series Firewall.

Troubleshooting

To test, if the connection is working, try to login as the user from another network host. When a user, for whom the authentication scheme applies, logs into the network, a log entry is created showing the login details such as source address, success or failure, time, etc. To access authentication logs, go to the **LOGS > Authentication Logs** page.

If the connection cannot be established:

- Make sure that you have entered the MSAD searching user in the **Searching User** field in the correct format: `user@domain`. Do not use the `domain\user` format.
- Verify that the entry for the **Base DN** where the lookup should be started does not contain spaces.
- Check the **Logs > Authentication Log** page for error messages when connecting to your Active Directory server.

Figures

1. ad01_67.png
2. ad02_67.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.